Thomas Kesselheim
Kurt Mehlhorn
Pavel Kolev

May 24, 2016
Deadline: lecture on May 30, 2016

Randomized Algorithms and Probabilistic Analysis of Algorithms

Summer 2016

Exercise Set 2

Exercise 1: (3+2 Points)
Suppose you shuffle n pieces of paper labeled by $1, \ldots, n$ in an urn and you draw one after the other without replacement.

(a) Show that in round i with probability $\frac{1}{i}$ you draw a number that is higher than any number before.

(b) What is the expected number of rounds in which you see a number that is higher than any number before?

Exercise 2: (4 Points)
Consider the following game. We start with an interval consisting of the numbers 1 to n. All numbers are initially white. In each round we choose a white number at random and recolor it black. The cost of the round is the length of the white interval containing the number. What is the expected cost of the game?
Hint: Run the game backwards.

Exercise 3: (4 Points)
A fair coin is flipped n times. For $1 \leq i < j \leq n$, let $X_{i,j}$, be 1 if the ith and jth flip landed on the same side; let $X_{i,j} = 0$ otherwise. Show that the $X_{i,j}$ are pairwise independent but not independent.

Exercise 4: (4 + 4 + 2 Points)
We study a randomized version of standard hashing. We want to store a set $S \subseteq \{0, \ldots, N-1\}$ in a table of size m. We use a function h that maps $\{0, \ldots, N-1\}$ to $\{0, \ldots, m-1\}$ and store an element x in the bucket $h(x)$.
Let $c \geq 1$ a constant. A family H of functions from $\{0, \ldots, N-1\}$ to $\{0, \ldots, m-1\}$ is called *c-universal* if for all x and y in $\{0, \ldots, N-1\}$ with $x \neq y$

$$\mathbf{Pr}_{h \in H}[h(x) = h(y)] \leq \frac{c}{m}.$$

(a) Assume that a set S is stored and we search for an element $x \notin S$. What is the expected number of elements in the bucket $h(x)$ if the hash function h is chosen randomly from a c-universal class?

Hint: For every $y \in S$, define a random variable X_y which is one if x and y are hashed to the same bucket and is zero otherwise.

(b) We now assume that $N = p$ is a prime. For $a, b, x \in \{0, \ldots, p-1\}$, let

$$h_{a,b}(x) = ((ax + b) \bmod p) \bmod m,$$

and let

$$H = \{\{h_{a,b} \mid 0 \leq a, b \leq p-1\}.$$

Show that H is $(\lceil p/m \rceil / (p/m))^2$-universal. For example, if $p = 97$ and $m = 8$ then $h_{23,73}(2) = ((23 \cdot 2 + 72) \bmod 97) \bmod 8 = 22 \bmod 8 = 6$.

(c) Mr. Fool believes that he can save one division and considers the functions

$$h_{a,b}(x) = (ax + b) \bmod m,$$

and the class

$$H' = \{h_{a,b} \mid 0 \leq a, b \leq p-1\}.$$

Let $K = \{0, m, 2m, \ldots, \lfloor p/m \rfloor m\}$. What happens when you hash K with one of the functions in H'? Is the class H' c-universal for some c?